ФОРМУВАННЯ ПЕРСОНАЛІЗОВАНОГО ОСВІТНЬОГО МОБІЛЬНОГО ОСВІТНЬОГО СЕРЕДОВИЩА НА ОСНОВІ КОНЦЕПЦІЇ BYOD

Івченко Є.І.,к.т.н., доцент, Божко В.І.

Зростання кількості мобільних пристроїв, поява нових додатків, зростання обсягу і цінності зберігаються на цих пристроях даних ставить перед навчальними закладами ряд нових питань:

- Що робити з мобільними пристроями співробітників та студентів?
- Як управляти контентом?
- Як забезпечити захист даних?

При цьому перед навчальними закладами постають такі проблеми:

- забезпечення централізованого управління налаштуваннями пристроїв під керуванням різних операційних систем (ОС);
- забезпечення безпеки інформації при її передачі та зберіганні;
- своєчасне оновлення програмного забезпечення;
- можливість використання як корпоративних пристроїв, так і пристроїв, які придбані користувачами;
- підтримка користувачів.

З точки зору організації електронного навчання впровадження концепції BYOD (Bring your own device) в практику навчального закладу знаменує собою фактичне створення персоналізованого мобільного освітнього середовища.

Впровадження принципів BYOD тягне за собою:

- збільшення мотивації і зацікавленості студентів;
- забезпечення розширеного доступу до освітніх ресурсів ВНЗ;
- забезпечення спільної навчальної діяльності студентів в аудиторіях.

Незважаючи на безліч виникаючих проблем, концепція BYOD (Bring your own device) завойовує все більше позицій в університетському середовищі. Тим часом, нові можливості неминуче пов'язані з новими небезпеками, і задля їх нейтралізації, навчальний заклад повинен приділяти більше уваги формуванню ефективного захищеного мобільного середовища на основі таких технологій як:

- Mobile Device Management (MDM) - управління мобільними пристроями;

- Virtual Desktop Infrastructure (VDI) - створення безпечних віртуальних робочих місць;
- Mobile DLP - протидія витокам інформації через мобільні пристрої.

Виділяють кілька ключових особливостей організації безпечного персонального мобільного середовища.

На етапі введення в експлуатацію це - контрольована активація доступу; управління конфігураціями (автоматичне поширення установок електронної пошти, VPN, Wi-Fi); корпоративний магазин додатків; регулювання поширення університетського контенту.

Безпечне управління мобільними пристроями як правила визначає: необхідність регулярної звітності і оповіщень; використання чітко визначених поштових серверів; єдине управління для всіх ОС; єдину консоль для всіх типів пристроїв; масштабовану архітектуру.

Захист даних при доступі до загальноуніверситетських ресурсів передбачає: розмежування доступу до ресурсів з боку корпоративної мережі; шифрування переданих даних; посилену автентифікацію; контроль даних, що завантажуються на пристрої.

Для нейтралізації виникаючих загроз виділяють наступні основні напрямки захисту:

- розробка та реалізація організаційних політик використання мобільних пристроїв;
- облік і управління пристроями;
- розмежування і контроль доступу до пристрою;
- захист критичних даних, що зберігаються або оброблюються на пристрої;
- автентифікація та захист даних при доступі до університетських ресурсів.

При цьому, облік і управління пристроями має на увазі інвентаризацію та облік пристроїв, моніторинг пристроїв, централізоване резервне копіювання, максимальну автоматизацію, використання групових налаштувань/політик.

Наразі все більше навчальних закладів намагаються ввести в організоване русло все різноманіття використовуваних студентами та співробітниками пристроїв шляхом централізованої установки MDM-додатків і як правило організоване таким чином персональне мобільне освітнє середовище дозволяє забезпечити ефективну реалізацію концепції BYOD в навчальному закладі.